AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
1606 STONEY LAKE DRIVE, FRIENDSWOOD, TEXAS

Case No. 3:19MJ007

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
a two-story, red and black brick house with white trim and gray shutters on the north side of Stoney Lake Drive facing southeast with the numbers 1606 are on a light gray brick inlaid into the masonry to the right of the front door.

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2261A(2)	Stalking

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

DeWayne Lewis
Applicant's signature

DeWayne Lewis, Special Agent
Printed name and title

Sworn to ~~before me and signed in my presence~~ telephonically.

Date: 1-17-19

Judge's signature

City and state: Galveston, Texas

Andrew M. Edison United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is 1606 Stoney Lake Drive, Friendswood, Texas 77546, further described as a two-story, red and black brick house with white trim and dark gray shutters. It is on the north side of Stoney Lake Drive facing southeast. The concrete driveway is on the right, which leads to the two-car garage attached to the east side of the house. The numbers 1606 are in a light gray brick laid into the masonry to the right of the front door.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 2261A, 2422(b), 2251, 2252 and 2252A, those violations involving Benjamen Slaughter and occurring after July 6, 2012, including:

a. Records and information relating to the Facebook account URL's: www.facebook.com/mastarslaughter, www.facebook.com/Sapphirerobertson, profile name "John Smith" or any other aliases, and/or User Account: 100025309980973;

b. Records and information relating to the identity or location of the suspect(s) or victim(s), including the minor victim known as AR;

c. Records and information relating to communications with Internet Protocol addresses
2600:100d:b021:af1c:ed4f:6129:ca68:fc51
2600:100d:b02c:cd6b:39cb:7082:21fa:0fda
2600:1700:4be0:8d40:35d3:f480:fc19:9726
2600:1700:4be0:8d40:4182:dfd9:61df:a57e and/or
99.50.124.77

d. Records and information relating to wiping, deleting or evidence-destroying software;

Records and information relating to the stalking, harassment, intimidation, online solicitation of minors and the possession, receipt, distribution or production of child pornography.

2. Computers or storage media used as a means to commit the violations described above, including desktop computers, laptop computers, smartphones, tablets, hard drives, thumb drives, compact discs, storage discs, memory sticks or any other items with electronic or digital storage capacity.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

d. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

i. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

k. evidence of the times the COMPUTER was used;

l. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

m. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

n. records of or information about Internet Protocol addresses used by the COMPUTER;

o. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF 1606 STONEY LAKE DRIVE, FRIENDSWOOD, TEXAS 77546	Case No. 3:19-mj-007

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, DeWayne Lewis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search 1606 Stoney Lake Drive, Friendswood, Texas 77546, hereafter referred to as the PREMISES. The residential PREMISES is more particularly described as a two-story, red and black brick house with white trim and dark gray shutters. It is on the north side of Stoney Lake Drive facing southeast. The concrete driveway is on the right, which leads to the two-car garage attached to the east side of the house. The numbers 1606 are in a light gray brick laid into the masonry to the right of the front door.

2. I am a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Homeland Security Investigations (HSI) office in Galveston, Texas. I have been so employed since June 2002. As part of my duties as an ICE Special Agent, I investigate criminal violations related to child exploitation and child pornography, including violations pertaining to online extortion and/or stalking, adults attempting to meet with juveniles for sexual encounters, and the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 875(d), 2422(b), 2251, 2252, 2252A and 2261A(2). I have received training in the area of child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have participated in the execution of numerous search warrants and covert operations involving child exploitation and the

online solicitation of minors, many of which involved child exploitation and/or child pornography offenses. I am in routine contact with experts in the field of computers, computer forensics, and Internet investigations. I annually attend the Dallas Crimes Against Children Conference where I attain various investigative training. I am currently a member of the Houston Metro Internet Crimes Against Children Task Force. This task force includes prosecutors and members of multiple police agencies across the southeast/coastal Texas and Houston metro regions.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and based on my conversations with other law enforcement officers involved in this investigation, or who have engaged in numerous investigations involving child exploitation and pornography. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 2261A, which makes it a crime to use any interactive computer service or electronic communication service or electronic communication system of interstate commerce to engage in a course of conduct that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person with the intent to harass, intimidate, or place under surveillance another person, have been committed by Benjamen Slaughter (aka: "John Smith," and aka: mastarslaughter) and are located at the PREMISES. There is also probable cause to believe that Benjamen Slaughter has an active, outstanding warrant issued for his arrest and he still resides at the PREMISES, as he did on September 22, 2017.

5. As a result of the investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of a crime, and other items illegally possessed in violation of federal law, including 18 U.S.C. §§ 2261A are present at the PREMISES and/or within the custody and control of Benjamen Slaughter (aka: John Smith and mastarslaughter). There is also probable cause to believe that the wanted felon, Benjamen Slaughter, currently resides and is harbored at the PREMISES.

6. This preliminary investigation involved a suspect, Benjamen Slaughter, storing images depicting child pornography in his Dropbox virtual storage account while he lived at the PREMISES. It also involved Slaughter soliciting at least one minor online for sexual contact. Further investigation identified at least two minor victims that were exploited by Slaughter. Follow-up investigation revealed Slaughter stalking one of the identified minor victims online via the internet through their respective Facebook social media accounts.

TECHNICAL TERMS

7. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. **IP Address:** The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). This design is known in the industry as "IPV4" version of internet protocol addresses. Every computer, and/or device attached to the Internet, must be assigned an IP address so that Internet traffic sent from, and

directed to, that computer may be directed properly from its source to its destination. When the internet was in its infancy there was an assumption that IPV4 would be sufficient to service the world's future IP Address needs. Over time it became clear this assumption was wrong and that the 4.3 billion IP addresses created with IPv4 would soon run out. The last remaining IPv4 Internet addresses were allocated by ICANN (the Global custodian and governing body of the Internet) in February 2011. The solution was to create a new version with many more addresses, which is what the internet industry has done with Version 6 (IPv6). The IPV6 versions of IP addresses resemble this one: 2602:30a:c00c:1c19:39be:c529:89aa:859. This transition, which has already begun, may take up to a decade or longer. The new version will create an almost limitless supply of IP addresses, in anticipation that nearly all technology in the future will be connected via the internet. Version 6 will have 3.4 billion-to-the-forth power IP addresses available for allocation. That is enough IP addresses for every single device utilizing this Protocol, virtually into perpetuity. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

9. **Facebook:** Facebook is a free-access social networking website of the same name available at URL: http://www.facebook.com and is accessible on desktop computers, laptop computers, tablets and smartphones. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts with their desktop, laptop, a tablet and/or smartphone to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses,

Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

10. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

11. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

12. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such

as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

13. Facebook allows users to upload photos and videos. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

14. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles. Such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a "chat" feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a "video calling" feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

15. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, etc.

16. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

17. Facebook Messenger, which is commonly referred to simply as "Messenger," is both a messaging application and a standalone platform on its own. It was originally developed as Facebook Chat in 2008, and underwent several variations and upgrades in the subsequent versions. It is commonly linked and recognized as an extension of the attributes of the Facebook user's profile, but can be downloaded as standalone iOS and Android apps on the user's tablet and/or smartphone. Users can send messages and exchange photos, videos, stickers, audio, and files, as well as react to other users' messages and interact with bots. The service also supports voice and video calling. The standalone apps support using multiple accounts, conversations with optional end-to-end encryption, and playing games.

18. **Apple, Touch ID and Face ID:** I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that

some models of Apple devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric, or alphanumeric, passcode or password. This feature is called Touch ID. More recently, iPhones and iPads offer the same unlock feature via facial recognition referred to as Face ID.

19. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center on the front of the device. In my training and experience, users of Apple devices that offer Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering the passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activities and thus has a heightened concern about securing the contents of the device.

20. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

21. In my training and experience, the person who is in possession of a device, or has the device among his or her belongings at the time the device is found, is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the PREMISES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID, or, if their Apple device is a more recent iteration, Face ID.

PROBABLE CAUSE

22. The Houston Metro Internet Crimes Against Children (ICAC) Task Force received information about suspicious activity from a cloud service company named Dropbox, Inc. Dropbox reported to the National Center for Missing and Exploited Children (NCMEC) on December 21, 2016, that someone was using their cloud services to store or transfer suspicious images via the internet. Dropbox viewed four files that were publicly available and provided those images to NCMEC. The report was forwarded to the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) Resident Agent in Charge office in Galveston, Texas. Special Agent DeWayne Lewis received and reviewed the report. There were approximately four suspicious files consisting of videos depicting nude minor females exposing

their genitals and engaging in sexual activity. The Dropbox customer information associated with the account was, in part:

Email Address:	slaughter_ben@yahoo.com
Screen/User name:	B S
IP Address:	99.25.91.11 on 08-05-16 at 02:28:11 UTC

23. Using law enforcement databases and online search tools, SA Lewis found that slaughter_ben@yahoo.com was associated with Benjamen Slaughter (DOB: 3/11/98) of Friendswood, Texas. His Texas Department of Public Safety driver's license indicated that his listed address was 1606 Stoney Lake Drive in Friendswood, Texas. On September 22, 2017, HSI Galveston and the Houston Metro Internet Crimes Against Children Task Force executed a federal search warrant at Benjamen Slaughter's residence at 1606 Stoney Lake Drive in Friendswood, Texas. During the execution of the warrant, agents made contact with Slaughter, who agreed to cooperate and answer questions. Although he was not under arrest, SA Lewis advised Slaughter of his Miranda warnings and he stated that he understood. Although Agents were there based on Slaughter's child pornography collection stored in his Dropbox account and the online coercion/enticement of a minor known to Slaughter as "Mandy," he described multiple scenarios where he had been in contact with minor females that he was trading nude images with. Those situations included a minor in Denton, Texas known as "Leah," whom he had known and exchanged nude images with for years. Another situation he described involved a minor from the nearby Clear Lake, Texas area known as "Amy," whom he had actually met and had sexual intercourse with. That minor victim eventually claimed that she was pregnant with his baby. Slaughter believed the baby's birthday would be April 4, 2017, placing conception in late June/early July of 2016. In that timeframe, the minor (DOB: 6/21/01) would have been 14 years old and Slaughter (DOB: 3/11/98) would have been 18 years old.

24. Slaughter's Apple iPhone was seized during the search warrant at his home and a forensic analysis was performed on it by Galveston Police Department Detective Garrett Groce, a member of the Houston Metro Internet Crimes Against Children task force. Detective Groce provided a report of the analysis to SA Lewis. Special Agent Lewis reviewed the report and found hundreds of text messages to various people that appeared to be, or claimed to be, minor females. Many of those conversations included sexually explicit demands by Slaughter. SA Lewis found multiple social media applications in the "services" section of the analysis. Those social media platforms included Skype, Facebook, Instagram, SnapChat, Skout and Text Free Ultra. The usernames for both his Skype and Skout accounts was "mastar123456789." The name, or word, "mastar," would be relevant later in the investigation.

25. Special Agent Lewis was able to isolate messages between Slaughter and the minor he knew as "Amy," hereafter referred to as "AR." Special Agents Lewis and Fornfeist interviewed AR with her guardian present on December 4, 2017, while she was 16 years old. AR stated that she met Slaughter via a dating app called "Skout," when she was 14 years old in eighth grade and he was an 18 year old senior in high school. They communicated via Skout and then via direct messaging on her phone. AR admitted that she exchanged and transmitted nude images of herself to Slaughter via multiple social media platforms and described situations where she would transmit nude images of herself to Slaughter via Snapchat from her backyard pool and from inside her shower. She explained that she was not comfortable providing the ones from inside the shower, but Ben was "being mean," so she acquiesced and sent him nude images. AR stated that their breakup was bad because she was moving further away from Slaughter's residence and he was upset because he would have to drive further to have sex with her. She described the situation as, "he was getting tired of it, and all he wanted to do was have sex."

26. Special Agent Lewis was contacted by AR's step-mother on November 7, 2018. She explained that she attempted to contact SA Lewis sooner, but had trouble locating his contact information. The victim's step-mother advised SA Lewis that Slaughter had made contact with AR, who was still a minor, via Facebook Messenger and may have anonymously sent flowers to her. Special Agent Lewis spoke with AR on November 12, 2018, and interviewed her about the circumstances surrounding Slaughter's latest contact with her. AR stated that she had been unexpectedly messaged by someone on/about August 27, 2018, at about 1:20 am using the profile name "John Smith" via Facebook Messenger. The person wrote, "this is Ben," in subsequent messages. The person also referred to her as "Sapphire," which was one of the nicknames that Slaughter called her, and convinced AR that it was indeed Ben Slaughter and not an imposter. AR asked Slaughter about his on-going investigation, and he replied that he had been "let off." AR stated that she became "pissed and worried" after Slaughter began inquiring about her infant daughter, Susan, and her paternity. AR was alarmed because she and Slaughter had broken up approximately three years ago around Thanksgiving and she didn't understand how Slaughter would have become aware that she had had a baby daughter. AR notified her step-mother about the messages from Slaughter later that same morning and told her that Slaughter had sent her a follow-up friend request through the "John Smith" Facebook profile at approximately 5:00 am. AR stated that Slaughter's "John Smith" Facebook profile displayed the image of a sloth as his profile photo. AR added that she received an anonymous delivery of flowers with an unsigned card at her residence during the August time period. The card made reference to AR being "my princess," and Slaughter had been the only person to reference her that way.

27. Special Agent Lewis conducted an online search for public Facebook profiles using the name "John Smith." Several John Smith profiles were located, including one with the image of

a sloth as the profile photo. The URL for that particular John Smith profile was www.facebook.com/mastarslaughter. Special Agent Lewis recognized the unique name of the profile (mastarslaughter), which was the combination of one of Slaughter's usernames in other accounts listed above (mastar) and his last name.

28. On December 17, 2018, SA Lewis had a federal search warrant issued to Facebook for messages in Slaughter's "John Smith" Facebook profile. Facebook responded by providing the requested information on January 15, 2019. The subscriber information included the following information, in part:

Account Identifier:	www.facebook.com/mastarslaughter
Name First	John
Last	Smith
Date Of Birth:	03/11/1998
Gender:	Male
Registration Date:	4-02-2018 19:08:58 UTC

29. The product information from Facebook also included messages, written using an electronic device, to and from minor victim AR. Even after AR stated that "this is scaring me," and "my stomach hurts," Slaughter continued to antagonize and threaten to pursue visitation and possible custody of AR's infant, which was born on/about January 7, 2018; three years after the two had separated. Excerpts from those messages are included below, in part:

8/31/18 05:33:09	AR	Why a sudden message This is scaring me
8/31/18 05:33:34	John Smith	I've tried messaging you before it never went through You blocked me remember
8/31/18 05:38:58	AR	My stomach hurts!
8/31/18 05:40:49	John Smith	If you had a child with someone else wouldn't you want to be in that child's life Wouldn't you want to be there for them
8/31/18 05:44:08	AR	Can we drop this

		Your engaged go be happy
8/31/18 05:44:50	John Smith	I can't knowing I'd never get to see my baby girl
8/31/18 05:45:07	AR	Yes you can Stay out of my happiness and my second chance You and your fiancee stay away from Susan
8/31/18 05:46:11	John Smith	I have rights to see her you know that You can't keep me from meeting her I can turn this into a custody fight and I promise you won't win
8/31/18 05:49:00	AR	Ben plz don't
8/31/18 05:49:19	John Smith	I'm trying to be nice about this
8/31/18 05:54:40	AR	I signed my parental rights away
8/31/18 05:55:24	John Smith	Well I didn't all it takes is a dna test and I can have my rights insteaded You know I have a really good lawyer for this kinda stuff she's the best in the country
8/31/18 05:57:53	AR	You will never find out where she's living Or who has adopted her
8/31/18 05:58:30	John Smith	I can also take you to court over that to Amy I had no idea what happened or what went on you did this behind my back there's ways to get things done Amy If your not going to help then I'm doing this my way
8/31/18 06:00:31	AR	Your fiancee will never be Susan roses mother
8/31/18 06:01:21	John Smith	But I'm not going to sit around and do nothing
8/31/18 06:01:30	AR	Ben drop it
8/31/18 06:02:26	John Smith	So like I send I'm going to do this my way
8/31/18 06:03:22	AR	You were almost put in jail For Dropbox nudes Of underage girls
8/31/18 06:04:15	John Smith	Like I send it was something that happened a long time ago something I tried getting rid of

30. Special Agent Lewis conducted surveillance at 1606 Stoney Lake Drive in Friendswood, Texas on January 3, 2019, and observed a red Chevrolet pickup bearing Texas license plate LLB4334 and a gold Infiniti SUV with a personalized license plate that read TAWNI. The LLB4334 registration returned to Slaughter's mother, Tawni Slaughter, at the PREMISES. The personalized plate appeared to be for Tawni Slaughter's lease on the Infiniti. Special Agents Lewis and Santiago Luna conducted surveillance at the PREMISES on January 16, 2019. The red Chevy

pickup left the residence at approximately 7:40 am and was operated by Benjamen Slaughter. Lewis and Luna followed the vehicle and watched as Slaughter, and an adult female passenger, vaped while he drove from the PREMISES and along S. Friendswood Drive. HSI Special Agent Kevin Fornfeist conducted surveillance at the residence on January 17, 2019, at approximately 1:00 am and observed the same red Chevy pickup in the driveway at the PREMISES.

31. On January 7, 2019, a federal arrest warrant (3:18-CR-27) was issued for Benjamen Slaughter charging him with Sexual Exploitation of Children and four other counts. As of the date of this affidavit, the arrest warrant had not been served on Slaughter.

Characteristics Common to Individuals with a Sexual Interest in Children

1. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the sexual exploitation of children which includes the distribution, receipt, possession and collection of child pornography:

a. Individuals with a sexual interest in children receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals with a sexual interest in children collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower, or "groom," the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with a sexual interest in children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, email account or in "virtual" storage, like in the iCloud or Dropbox.com. Individuals with a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

   i) "Child erotica," as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

d. Likewise, Individuals with a sexual interest in children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area or "virtual" storage. These collections are often maintained for several years and are kept close by, or remotely accessible, usually at, or via, the collector's residence, to enable the collector to view his collection, which is highly valued.

e. Individuals with a sexual interest in children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of

individuals with whom they have been in contact and who share the same interests in sex with children or child pornography.

f. Individuals with a sexual interest in children prefer not to be without their child pornography, or prohibited from its' access, for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

2. Based upon my training, knowledge and experience in investigations related to child exploitation and my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography and exploitation, I am aware that individuals who access paid subscription or free sites offering images and/or videos depicting child pornography do so for the purpose of downloading or saving these images to their hard drive or other storage media so that the images and videos can be added to their collection. I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet such as newsgroups and websites, and via paid subscriptions, as well as their own "trophy photos" of sexual conquests involving the exploitation of children. Those trophy photos usually consist of photos they've produced of a live victim they've touched or a screen capture of a victim they've exploited online.

3. Additionally, based upon my training, knowledge and experience in investigations related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes have a collection of child pornography and will ask children to take and send naked images of the themselves that would constitute child pornography as well as child erotica.

4. Furthermore, based upon my training, knowledge and experience in investigations

related to child exploitation and child pornography cases, I am aware that individuals who have a sexual interest in children will oftentimes utilize social media such as Snapchat, Instagram, Kik Messenger, Twitter, Facebook, WhatsApp, ChatStep, Skout, Grindr, Craigslist and other online services to meet and communicate with minors. Individuals with a sexual interest in children know that social media allows for seemingly anonymous communication which they can then use to groom the minors and set up meetings, whether in person or online, in order to sexually exploit them.

Computers and Child Pornography

5. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology (including advances in smartphones, tablets and internet connectivity) have revolutionized the way in which children are exploited and how child pornography is produced, distributed, and utilized. Advancements in cellular telephone technology and mobile applications have furthered those revolutionary methods of exploitation.

6. Cellular telephones are routinely connected to computers to re-charge the batteries and synchronize the mobile telephone with their matching computer programs, or "applications," on the computer. Cellular telephones are connected to the user's computer to transfer, save or back-up files or to download files, programs or "applications" via the internet, as one would do for music or ring tones. Users connect their cellular telephones to their computer to save, or back-up, their content or upload those files via the internet to a virtual storage medium like the iCloud or Dropbox, which allow users to access that content from any device with internet access, including their mobile devices (cellular phones or tablets) or another computer. Users can also download programs to their computers that mimic, or operate as if they are using, applications on their cellular

telephone. Some of those examples include "iPadian," "Andy," and "BlueStacks." People with a sexual interest in children have embraced these technologies in their efforts to exploit children, conceal their true identities, misdirect investigators, hide evidence and communicate with others with the same interests.

7. Technologies for portable cellular telephones, their batteries, internet connectivity and quick-charge devices have also greatly advanced. Today's vehicles often advertise built-in options for internet connectivity. In early 2013, General Motors announced it would partner with AT&T to outfit most of its 2014 models with high-speed data connectivity, with those same options available from Chrysler, Audi and Ford. These portable devices are commonly stored and used in vehicles and derive their power from being plugged in to cigarette lighters or auxiliary power outlets. Other portable navigation devices, like the Garmin or TomTom, provide turn-by-turn directions to previously unknown locations when the user inputs the desired address or destination and are commonly kept or stored in the user's vehicle. Many modern vehicles are equipped with satellite navigation from the factory. Modern computer technology in today's vehicles can navigate you to your destination, synchronize your cellular telephone to the on-board monitor for hands-free use and adjust radio and environmental controls by responding to voice-activated commands. The suspects' vehicles have increasingly become mobile storage places for evidence like the satellite navigation devices, laptops or storage media concealed from other household members. They also can hold other evidence linked to their travel for contact with like-minded adults and sexually exploited minors; like gasoline, toll booth and parking receipts or traffic tickets.

8. Prior to the advent of computers and the internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of images. To distribute these

images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computer technology and the Internet, producers, collectors and distributors of child pornography can instantly and remotely upload images into virtual storage, like in the iCloud or Dropbox, allowing them to operate almost anonymously.

9. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers (including cellular telephones) and wi-fi technology has also revolutionized the way in which those who seek child pornography are able to obtain this information. Computers, and the modern "smartphone," allow simplified, often anonymous communication with persons far-removed from the solicitor. They can communicate with others with similar interests or where laws against sex with children are more lax or less enforced. They can also communicate directly with minor victims in a safe environment believing that their communications are anonymous. Computers also serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development and advancement of computers and internet technology has changed the methods used by those who seek to sexually exploit children and obtain access to child pornography in these ways.

10. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, including cameras contained in the latest smartphones. A digital camera can be attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in

ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. Because of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

11. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as Comcast, AT&T and America Online ("AOL"), which allow subscribers to dial a local number or otherwise directly connect to a network, which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

12. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in sex with children or child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to

child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache[1] to look for "footprints" or "relics" of the websites and images accessed by the recipient.

13. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single compact disk can store thousands of images and pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes and larger are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

14. Computer files, or remnants of such files, can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is - in space

[1] "Cache" refers to text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CONCLUSION

33. Based upon my own knowledge, experience and training related to child pornography and child exploitation investigations, I am aware that individuals who have a sexual interest in children who possess and/or distribute child pornography are often child pornography collectors. They often collect, or hoard, their images for the purposes of trading with others as a method of adding to their own vast collections. Furthermore, I know that individuals with a sexual interest in children and who are involved in the collection and distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet, such as in newsgroups and other websites, including via paid-subscription sites. Sometimes those "payments" are in the form of new, or bartered, images depicting the sexual exploitation of a child.

34. Finally, based upon the conduct of individuals who have a sexual interest in children, who possess and collect child pornography, and who hoard, receive and distribute child pornography, namely, that they tend to maintain their collections for long periods of time, even over the course of years, there is probable cause to believe that evidence of the offenses of Receipt,

Distribution and Possession of Child Pornography is currently located at the PREMISES. I believe the suspect has demonstrated these offender characteristics based on his use of the internet to manipulate child exploitation material and his posting of multiple child pornography images onto his blog for other users to view, save or share.

35. Based on the above information, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 2252 and 2252A, which, among other things, makes it a federal crime for any person to possess, receive or distribute child pornography, have been violated, and that any such property is evidence of a crime, fruits of a crime, contraband and other items illegally possessed and is located at the PREMISES occupied, maintained, and/or controlled by Benjamen Slaughter.

Respectfully submitted,

DeWayne Lewis
Special Agent
DHS/ICE/Homeland Security Investigations

Subscribed and sworn to ~~before me~~ telephonically on January 17, 2019

The Honorable Andrew M. Edison
UNITED STATES MAGISTRATE JUDGE